LISTING OF CLAIMS

1. **(Currently Amended)** A method of controlling access to a network, the method comprising:

configuring an authentication server to include a first location information corresponding to a combination of identities of a user and of a mobile client of the user, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server is coupled to the network and comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

requesting by a network switch the combination of identities of the user and of the mobile client of the user attempting to connect to the network;

receiving, by the authentication server, the combination of identities of the user and of the mobile client of the user via the network switch;

associating, by the network switch, a second location information corresponding to the mobile client with the combination of identities of the user and of the mobile client of the user, wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect;

storing the second location information on the network switch;

periodically downloading, by the network switch, at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device;

authenticating, by the authentication server, the combination of identities of the user and of the mobile client of the user received by the authentication server;

comparing, by the authentication server, the second location information corresponding to the mobile client against the first location information from the VSA;

deciding, by the authentication server, whether to grant or deny access to the network for the mobile client in response to authenticating the combination of the identities of the user and of the mobile client of the user, wherein the deciding is in response to comparing the second location information against the first location information; and

informing the network switch by the authentication server whether to grant or deny access to the network for the mobile client.

2-3. (Cancelled).

4. (Previously Presented) The method of claim 1, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared encryption key, a smart card identifier, and any combination of the foregoing information.

5. (Previously Presented) The method of claim 1, wherein the edge device is capable of providing one or more wireless devices an access point for connecting to the network.

6. (Previously Presented) The method of claim 1, wherein the mobile client is a wired device capable of connecting to the network through an Ethernet switch port.

7. (Previously Presented) The method of claim 1, wherein authenticating the combination of identities of the user and of the mobile client of the user comprises authenticating the identity of the mobile client via a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing.

8. (Cancelled).

9. (Cancelled)

10. (Previously Amended) A network system comprising:

a network;

an authentication server coupled to the network, the authentication server configured to include a first location information corresponding to a combination of identities of a user and of a mobile client of the user, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

a network switch coupled to the network and having an authenticator for requesting the combination of identities of the user and of the mobile client of the user and for associating a second location information corresponding to the mobile client with the combination of the identities of the user and of the mobile client of the user, wherein the mobile client is operable to communicate to the authenticator of the network switch, and wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect; and

a network manager comprising an application running on a server, wherein the application permits a network administrator to create and update a policy table of the authentication server, wherein the network manager operable to:

store the second location information on the network switch;

periodically download at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device;

wherein the authentication server is operable to:

authenticate the combination of the identities of the user and of the mobile client of the user received by the authentication server;

compare the second location information corresponding to the mobile client against the first location information from the VSA;

decide whether to grant or deny access to the network for the mobile client in response to authenticating the combination of the identities of the user and of the mobile client of the user and in response to comparing the second location information against the first location information; and

inform the network switch whether to grant or deny access to the network for the mobile client.

11-12. (Cancelled).

13. (Cancelled)

14. (Previously Presented) The network system of claim 10, wherein the edge device is a wireless access point.

15. (Previously Presented) The network system of claim 14, wherein the mobile client is capable of connecting to the network through the wireless access point of the edge device.

16. (Previously Presented) The network system of claim 10, wherein the mobile client is a wired device capable of connecting to the network switch through an Ethernet port.

17-18. (Cancelled).

19. (Previously Presented) The network system of claim 10 further comprising an interface for permitting an administrator to associate the second location information to the mobile client.

20. (Original) The network system of claim 10, wherein the authentication server is included in a network switch.

21-23. (Cancelled).

24. (Previously Presented) The network system of claim 10, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

25. (Previously Presented) The network system of claim 10, wherein the network switch comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

26. (Previously Presented) The network system of claim 10, wherein the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

27-38 (Cancelled).

39. **(Currently Amended)** A network system for controlling access to a network, the network system comprising:

means for configuring an authentication server to include a first location information corresponding to a combination of identities of a user and of a mobile client of the user, the first location information being a location at which the mobile client is permitted to connect to the network,

wherein the authentication server is coupled to the network and comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes, and

wherein the first location information is included within a RADIUS vendor specific attribute (VSA) of the RADIUS attributes;

means for requesting by a network switch the combination of the identities of the user and of the mobile client of the user from the mobile client attempting to connect to the network;

means for receiving, by the authentication server, the combination of the identities of the user and of the mobile client of the user via the network switch;

means for associating, by the network switch, a second location information corresponding to the mobile client with the combination of the identities of the user and of the mobile client of the user, wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect;

means for storing the second location information on the network switch;

means for periodically downloading, by the network switch, at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device;

means for authenticating, by the authentication server, the combination of the identities of the user and of the mobile client of the user received by the authentication server;

means for comparing, by the authentication server, the second location information corresponding to the mobile client against the first location information

means for deciding, by the authentication server, whether to grant or deny access to the network for the mobile client in response to authenticating the combination of the identities of the user and of the mobile client of the user and in response to comparing the second location information against the first location information; and

means for informing the network switch by the authentication server whether to grant or deny access to the network for the mobile client.

40. (Previously Presented) The network system of claim 39, wherein the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

41. (Previously Presented) The network system of claim 39, wherein the mobile client is a wireless device capable of connecting to the network through an access point.

42. (Previously Presented) The network system of claim 39, wherein the mobile client is a wired device capable of connecting to the network through an Ethernet port.

43. (Previously Presented) The network system of claim 39, wherein the means for authentication includes:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

44-45. (Cancelled).

46. (Previously Presented) The method of claim 1, wherein the mobile client is associated with a newly located access point upon authenticating the combination of the identities of the user station and of the mobile client and determining, by comparing an updated location information corresponding to the mobile client against the first location information in the policy table, the first location information being the information that the mobile client is still authorized to access the network.

47. (Cancelled).

48. (Previously Presented) The method of claim 1, wherein the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect.

49. (Previously Presented) The network system of claim 10, wherein the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect.

50. (Previously Presented) The network system of claim 24, wherein the identity of the mobile client includes a smart card identifier.

51. (Cancelled).

52-53. (Cancelled)

54. (Previously Presented) The method of claim 1, wherein the user identity comprises user name.

55. (Previously Presented) The network system of claim 10, wherein the user identity comprises user name.

56. (Previously Presented) The network system of claim 39, wherein the user identity comprises user name.

57. (**New**) The method of claim 1 further comprises:

downloading to the mobile client or the edge device sensitive information when the mobile client is granted access to the network.

58. (**New**) The method of claim 57 further comprises:

erasing the sensitive information when the mobile client or the edge device is denied access to the network.

59. (**New**) The method of claim 1 further comprises:

bypassing authenticating of the combination of identities of the user and of the mobile client of the user when the mobile client moves to another location on the network.

60. (**New**) The method of claim 59 further comprises:

in response to bypassing authenticating, applying information about the other location to grant or deny access to the network for the mobile client of the user.